**Příloha č. 1 smlouvy o dodávce a instalaci dlouhodobého důvěryhodného úložiště**

**TECHNICKÁ SPECIFIKACE DŮVĚRYHODNÉHO DATOVÉHO ÚLOŽIŠTĚ
(dále jako „DDÚ“)**

Dodavatel výslovně prohlašuje, že DDÚ splňuje veškeré níže uvedené technické požadavky:

 **Základní nebo obecné funkcionality**

P.1 Soulad s legislativou pro dlouhodobé uložení zdravotnické dokumentace v souladu s legislativou a dalšími požadavky uvedenými v tomto dokumentu a princip zajištění důvěryhodnosti elektronicky uložených nebo jinak zpracovávaných dokumentů musí být v souladu s nařízením EU eIDAS (nařízení EU č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu.)

P.2 DDÚ bude podporovat formáty AdES (PAdES, CAdES, XAdES) a ASIC kontejnery.

P.3 Komponenta pro Dlouhodobé Důvěryhodné Ukládání bude sloužit jako repozitář zdravotnické dokumentace (DocRep) pro důvěryhodné dlouhodobé ukládání zdravotnické dokumentace. Tento systém umožní informačním systémům uložit elektronicky podepsanou zdravotnickou dokumentaci do centrálního důvěryhodného úložiště. Na základě požadavku obsahujícího identifikátor dokumentu zprostředkuje služba poskytnutí dokumentu z archivu a zprostředkuje důkazy o důvěryhodnosti. Služby DEA prostřednictvím ESB budou poskytovat údaje o skartované dokumentaci řízeným skartačním procesem.

P.4 Řešení musí být plně v souladu s platnou legislativou ohledně vedení zdravotnické dokumentace v elektronické podobě a ochrany osobních údajů (viz jiné části tohoto dokumentu).

P.5 DDÚ musí vůči okolním systémů systémům vystupovat jako CAS, tj. musí každému uloženému dokumentu přiřadit jedinečné a neměnné ID, pomocí kterého bude dokument identifkován v rámci IS organizace.

P.6 DDÚ musí umožňovat ukládat různé typy všech dokumentací (zdravotnické a DDÚ zdravotnické dokumentace), minimálně v rozsahu spisového a skartačního řádu organizace.

P.7 DDÚ musí podporovat ukládání a zpřístupňování dokumentace ve formě textových, grafických, audiovizuálních, digitálních nebo jiných obdobných záznamů.

P.8 Systém obsahuje uživatelské rozhraní pro přístup k uložené dokumentaci provozované ve webovém prohlížeči bez nutnosti instalovat přídavné moduly či rozšíření. Toto uživatelské prostředí umožňuje vyhledávání dle různých vyhledávacích kritérií, např. dle pacienta, klinické události apod.

P.9 Dlouhodobé zajištění integrity archivovaných dokumentů i na úrovni datového úložiště po dobu technické životnosti úložiště. Možnost budoucí migrace na nové datové úložiště plnící podmínky kladené na takové úložiště bez ztráty integrity archivovaných dokumentů a zajištění integrity archivovaných dokumentů na další období.

P.10 Systém musí umožňovat také řízenou skartaci postavenou dle platných předpisů, která na základě metadat určují životnost dokumentu a termín jeho skartace a dále protokoly o uskutečněných skartacích.

P.11 Systém musí umožňovat nastavení a řízení přístupových práv dle rolí uživatele a jeho organizačního zařazení.

P.12 Systém DDÚ nesmí být licenčně omezen na počet nebo typ připojených produkčních systémů nebo přístrojů; typ archivované dokumentace; počet uživatelů nebo zobrazovacích stanic.

P.13 Systém umí dynamicky reagovat na dodatečné informace, které mohou dodatečně ovlivnit a změnit skartační plán a zohlednit tyto změny do skartační lhůty pro konkrétní archivované dokumenty.

P.14 Systém DDÚ musí zahrnovat uživatelské rozhraní pro přístup k dokumentaci provozované ve webovém prohlížeči bez nutnosti instalovat přídavné moduly či rozšíření.

P.15 Systém DDÚ musí umožňovat rozšíření v budoucnu zvýšení výkonu formou škálování aplikačních serverů rozšíření aplikačních serverů stávajícího úložiště, nikoliv dodávkou dalšího.

P.16 Auditování a logování provozu jednotlivých prvků systému a možnost vyhodnocování min. 1 rok zpětně a logy musí být důvěryhodně pečetěny a uloženy.

P.17 Aplikační servery musí podporovat běh ve vysoké dostupnosti v režimu Active Active a Active-Pasive ve dvou lokalitách a loadbalacing na úrovni aplikačních serverů

P.18 Systém musí podporovat multitenantní konfiguraci, tj. pro různé typy dokumentů, tj. musí jít v rámci jedné instance vytvořit zcela samostatně konfigurovatelné úložiště jak z pohledu metadat, uživatelských oprávnění a dalších parametrů zajišťující možnost ukládání zdravotnické i nDDÚravotnické dokumentace.

P.19 DDÚ musí používat úložiště MS SQL nebo PostreSQL.

P.20 Nad rámec běžného pečetění při zpracování dokumentů, musí v rámci svého integračního rozhraní poskytovat funkcionalitu Pečetění – Opečeť pro dokumenty ve formátech AdES a ASIC kontejnery.

P.21 DDÚ nesmí být omezen množstvím uložených dat, počtem integrovaných systémů původců dat ani počtem uživatelů přistupujících přímo nebo prostřednictvím dalších systémů k DDÚ.

**Požadavky národního standardu (NSeSSS)**

P.22 Systém dlouhodobé a důvěryhodné uložení elektronických dokumentů podle zákona č. 499/2004 Sb., o archivnictví a spisové službě, Národního standardu pro elektronické systémy spisové služby (NEeSSS) a podle úrovně technického řešení problematiky obvyklého v Evropské unii v platném znění.

P.23 DDÚ umožňuje službu autorizované konverze, která umožňuje konvertovat PDF/A dokument do papírové formy.

P.24 DDÚ umožňuje řízený proces skartace dle platné vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci (viz přílohy č. 2 a 3 této vyhlášky), vytvoření skartačního návrhu na základě skartačního plánu, skartačních znaků a skartačních lhůt.

P.25 DDÚ vede transakční logy o všech operacích s možností exportu logů do externího SIEM systému. Veškeré přístupy k datům a aktivita uživatelů jsou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů. V systému je evidována jednoznačná identifikace kdo, kdy provedl zápis do systému nebo provedl náhled.

P.26 DDÚ podporuje práci se SIP balíčky

P.27 DDÚ podporuje kompletní režim skartace dle 499/2004 a NSeSSS.

P.28 DDÚ podporuje režim spisovna dle 499/2004 vč. zápůjček, skartačních návrhů apod.

**Služby vytvářející důvěru (konektory)**

P.29 Musí obsahovat konektor alespoň na jednoho kvalifikovaného poskytovatele služeb vytvářejících důvěru zajišťující kvalifikované pečetění a uvedeného na stránkách Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru - Ministerstvo vnitra České republiky (mvcr.cz)

P.30 Musí obsahovat konektor alespoň na jednoho kvalifikovaného poskytovatele služeb vytvářejících důvěru zajišťující službu Kvalifikovaného ověřování platnosti kvalifikovaných elektronických podpisů a pečetí a uvedeného na stránkách Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru - Ministerstvo vnitra České republiky (mvcr.cz)

P.31 DDÚ musí nativně podporovat, obsahovat konektor, alespoň jeden kryptografický prostředek pro ukládání elektronických podpisů a pečetí (HSM) uvedený na seznamu SSCD a QSCD zveřejňovaném Evropskou komisí (Compilationof Member States notification on SSCDs and QSCDs).

P.32 Nad rámec standardních validačních mechanismů musí na integračním rozhraní DEA poskytovat funkci pro všechny formáty AdES a ASIC kontejnery a „zvaliduj a vrať“ kde výstupem je validační report v podobě PDF nebo XML

P.33 DDÚ bude na svém rozhraní poskytovat metody pro vzdálení podepisování a pečetění (pro účely tohoto funkčního požadavku se za vzdálené podepisování nebo pečetění považuje situace, kdy uživatel nemá svůj token nebo vlastní úložiště a využívá pro podepisování nebo pečetění síťový kryptografický prostředek nebo služeb některého z kvalifikovaných poskytovatelů zajišťující službu vzdáleného pečetění nebo podepisování)